INSTAURER LA CONFIANCE À L'ÉGARD DU COMMERCE ÉLECTRONIQUE :

Cadre pour l'authentification électronique au Canada

Le présent document a été préparé par la
Direction générale du commerce électronique
Industrie Canada
Juillet 2000

Ce document ainsi que d'autres documents sont offerts par voie électronique sur le Web (**http://e-com.ic.gc.ca/**).

Also available in English under the title: *Building Trust and Confidence in Electronic Commerce: A Framework for Electronic Authentication in Canada*

Au sujet du présent document

Le présent document a été préparé par la Direction générale du commerce électronique d'Industrie Canada (qui s'appelait auparavant Groupe de travail sur le commerce électronique), dans le cadre de ses travaux visant à soutenir le leadership du Canada dans le domaine du commerce électronique. Il répond au besoin de créer un climat de confiance au sein de l'économie numérique mondiale qui se dégage de la stratégie canadienne sur le commerce électronique. Il s'inscrit dans le programme de consultation en cours auprès des principaux intervenants[1] au sujet de la manière dont on pourrait développer des services d'authentification et de certification au Canada.

En octobre 1998, le gouvernement du Canada a annoncé sa politique en matière de cryptographie et indiqué qu'il ne réglementerait pas les entités du secteur privé fournissant des services d'authentification et de certification. La Direction générale du commerce électronique a par la suite entrepris un programme de consultation pour discuter avec les intervenants de la manière dont le secteur privé pourrait développer des services d'authentification et de certification au Canada et pour déterminer si des obstacles freinent l'investissement dans ces services ou leur utilisation.

Pour le moment, on a terminé une série de discussions bilatérales. Cette ronde préliminaire de consultations a indiqué qu'un dialogue soutenu entre le secteur public et le secteur privé était nécessaire et qu'un grand nombre des questions devront être étudiées conjointement.

Après ces consultations bilatérales, on a tenu en décembre 1999 un atelier qui a réuni un groupe plus vaste d'intervenants en vue de mieux faire comprendre les occasions et les défis inhérents à la création et à la mise en oeuvre de ces services au Canada et pour déterminer quelles mesures les secteurs privé et public pourraient prendre pour profiter des occasions et relever les défis. Les intervenants étaient d'accord pour dire qu'il faudrait tenir compte des vues d'un groupe plus important et préparer un document de consultation qui propose l'élaboration d' un cadre pour assurer la progression des travaux.

Le présent document décrit les services d'authentification et de certification et donne certaines informations sur les politiques actuelles. On y indique qu'une approche coordonnée est nécessaire et on y propose l'établissement d'un cadre pour ces services. Ce cadre devra prendre en compte les dimensions internationales.

L'approche d'Industrie Canada a consisté à utiliser des paramètres de haut niveau pour définir les services d'authentification et de certification, compte tenu du fait que les intérêts du

---

[1] Au nombre des intervenants, on compte des représentants du secteur privé, des groupes de consommateurs et certaines provinces. Voir l'***Appendice A*** qui contient une liste complète. Pour en savoir davantage sur les divers éléments du programme de consultation, voir **(http://e-com.ic.gc.ca/francais/authen/631e10.html)**.

gouvernement fédéral résident principalement dans certains aspects politiques généraux des services d'authentification. De plus, Industrie Canada, reconnaissant que différentes applications peuvent exiger des solutions différentes, a décidé d'adopter une approche neutre au point de vue technologie et architecture. Cette approche n'est pas focalisée sur une solution spécifique en matière de sécurité.

Toutefois, le présent document traite particulièrement de certains aspects liés aux signatures électroniques compte tenu du rôle prédominant que joue la cryptographie à clé publique dans cet environnement émergent. Les futurs travaux régleront les problèmes liés aux techniques qui remplaceront la cryptographie à clé publique au fur et à mesure qu'elles sont mises au point.

Le présent document situe les résultats des consultations tenue par la Direction générale. Il contient aussi des éléments du Bureau de la consommation et du Bureau de la politique de concurrence, ainsi que du Secrétariat du Conseil du Trésor. Les propositions qu'il contient soulèvent des questions importantes en ce qui a trait au développement et à l'utilisation des services d'authentification et de certification au Canada, au sujet desquels Industrie Canada cherche à obtenir des points de vue diversifiés.

Les intervenants ont déterminé qu'un dialogue soutenu entre le secteur public et le secteur privé était essentiel à l'instauration d'un climat de confiance au Canada. La prochaine étape de ce dialogue consistera à inciter les intervenants à répondre à n'importe laquelle ou à toutes les questions qui figurent dans les diverses parties du présent document. L'***Appendice C*** a été élaborée pour offrir un point de référence unique sur les questions pour lesquelles on cherche à obtenir des opinions et des contributions. On demande aussi des contributions relatives au sommaire des rôles éventuels figurant dans l'***Appendice D***.

On reconnaît également que, comme le présent document couvre une large gamme de questions et de sujets, les intervenants peuvent choisir de répondre uniquement aux questions qui les intéressent.

Pour tout complément d'information au sujet du contenu du présent document et du processus de consultation, ou pour soumettre des commentaires au sujet du document, veuillez communiquer avec :

Peter Ferguson
Directeur, Politiques en commerce électronique
Direction générale du commerce électronique
Industrie Canada
300, rue Slater, 20e étage
Ottawa (Ontario) K1A 0C8
Courriel : **authen@ic.gc.ca**
Télécopieur : (613) 941-0178

Prière de nous faire parvenir les commentaires au plus tard le **21 septembre 2000.**

Vos remarques sur l'approche proposée dans le présent document et d'autres questions apparentées sont une étape essentielle à la continuité d'un bon dialogue sur ce sujet.

TABLE DES MATIÈRES

Introduction et portée 1
- a) Contexte 1
- b) Stratégie et programme du Canada en matière de commerce électronique 1
- c) Cryptographie 2
- d) Définition des services d'authentification et de certification 3

Partie 1 - Contexte 6
- 1.1 Cadre politique actuel en vue d'instaurer la confiance 6
  - a) Protection du consommateur 6
  - b) Protection des renseignements personnels 6
  - c) Cadre juridique 7
  - d) Sécurité 8

Partie 2 - Définition d'un programme pour l'avenir 9
- 2.1 Constatations des intervenants 9
  - a) Nécessité d'un cadre 9
  - b) Compatibilité nationale 9
  - c) Compatibilité internationale 10
  - d) Dimensions liées à la concurrence 12
  - e) Aspects liés au développement des marchés 13
- 2.2 Portée proposée du cadre 13

Partie 3 - Un cadre pour les services d'authentification et de certification- Approche proposée 15
- 3.1 Généralités 15
- 3.2 Principes 15
  - a) Généralités 15
  - b) Applicabilité et portée 17
  - c) Teneur 18
  - d) Respect 19
  - e) Rôle des AC du secteur public (en particulier l'ICP-GC) 20
  - f) Mécanisme d'élaboration des principes 21
- 3.3 Principes de base de l'accréditation 22

Partie 4 - Développement des marchés : possibilités et défis 24
- 4.1 Promouvoir l'adoption et l'utilisation 24
  - a) Investissement stratégique 24
  - b) Sensibiliser les consommateurs au commerce électronique et les inciter à l'utiliser 26
  - c) Favoriser la concurrence et l'innovation 28

Partie 5 - Conclusions et prochaines étapes 30
- 5.1 Prochaines étapes proposées 30

Programme de consultation sur l'authentification :
Intervenants participant ..... Appendice A

Cadre proposé en vue de la discussion sur le ou les modèles d'accréditation ..... Appendice B

Liste récapitulative des questions ..... Appendice C

Sommaire des rôles éventuels des secteurs public et privé ..... Appendice D

Liste des abréviations

Sources choisies

Introduction et portée

a) Contexte

Il y a peu de temps encore, la plupart des transactions en ligne étaient limitées au domaine privé ou à des groupes fermés de partenaires commerciaux ou de clients connus les uns des autres. L'existence d'un lien de droit entre les participants à ces modèles signifie que les relations entre les parties sont relativement bien comprises et présentent un cadre d'analyse prévisible. Ce n'est pas le cas dans le domaine public, dans des environnements ouverts (comme Internet), où les parties sont étrangères les unes aux autres et n'ont pas conclu directement d'ententes ni de contrats. Il peut aussi y avoir des intermédiaires. Les relations complexes qui peuvent en résulter ont suscité des questions nouvelles. Il faut donc examiner des solutions qui peuvent instaurer la confiance dans les cas où des parties qui n'étaient pas en relation au préalable communiquent et font des transactions.

La cryptographie est importante pour instaurer la confiance à l'égard des marchés électroniques puisqu'elle permet à des parties qui ne se connaissent pas d'échanger et d'authentifier de l'information, tout en faisant des affaires en ligne en toute sécurité. Les services liés à la cryptographie faisant intervenir des mécanismes d'authentification et de certification et offrant cette fonctionnalité font partie intégrante du programme visant à instaurer la confiance à l'égard du commerce électronique à grande échelle.

Il existe une grande variété de technologies et de mécanismes pour authentifier et certifier les transactions électroniques, ainsi qu'un certain nombre de modèles architecturaux différents pour les administrer. Les différents types de transactions exigent des solutions différentes et le choix de la technologie est déterminé par les applications et les parties en cause. De nouvelles solutions et approches font chaque jour leur apparition. Le marché qui évolue avec ces services est donc dynamique et diversifié.

Les consultations des intervenants menées jusqu'à maintenant ont permis de formuler la conclusion suivante : la concurrence et l'innovation joueront un rôle important dans ce marché. Toutefois, la nécessité d'instaurer la confiance à l'égard des services d'authentification et de certification est aussi importante que celle de promouvoir la concurrence et de favoriser l'innovation.

b) Stratégie et programme du Canada en matière de commerce électronique

En septembre 1998, le Premier ministre a annoncé la *Stratégie canadienne sur le commerce électronique*[2] et présenté une vision de l'avenir du Canada dans le domaine du commerce électronique. La stratégie fait état d'un certain nombre de mesures à prendre en priorité, notamment susciter la confiance dans l'économie numérique.

---

[2] Voir le site **http://e-com.ic.gc.ca/francais/60.html** pour obtenir de l'information sur les diverses initiatives qui font partie de cette stratégie.

Alors que l'objectif du programme *Un Canada branché*[3] est de faire en sorte que le Canada compte parmi les chefs de file dans la connectivité mondiale[4], l'accès fournit seulement le moyen de participer au marché mondial du commerce électronique. Le gouvernement reconnaît que cela se traduira par de véritables possibilités seulement si nous sommes aussi en mesure de remplir les conditions nécessaires en vue d'instaurer la confiance dans le marché électronique.

Le discours du Trône d'octobre 1999 indique que le gouvernement prendra des mesures pour « faire du Canada un centre d'excellence en commerce électronique et encourager son utilisation dans l'ensemble de l'économie ». Plus récemment, dans un rapport préparé par la Table ronde sur les possibilités des affaires électroniques canadiennes[5], on reconnaît la position de leader que le Canada a acquise sur la scène nationale et internationale. Toutefois, les auteurs du rapport indiquent que le Canada doit aussi faire preuve de dynamisme pour saisir toutes les possibilités offertes par le commerce électronique ou risquer de prendre du retard par rapport aux autres économies avancées. Il est essentiel d'instaurer la confiance dans l'économie numérique pour saisir ces possibilités.

c) Cryptographie

Les techniques de cryptographie peuvent être utilisées comme fondement pour instaurer la confiance dans l'économie numérique étant donné qu'elles ***sauvegardent*** l'information, ***protègent*** les communications et ***authentifient*** les parties aux transactions. Plus précisément, elles peuvent être utilisées pour mettre au point des ***signatures numériques***[6] qui assurent :

i) ***l'authentification*** - preuve que les utilisateurs sont bel et bien ceux qu'ils prétendent être (ou que l'identité des ordinateurs, logiciels, etc. est valide);

---

[3] *Un Canada branché* constitue la vision et le plan du gouvernement fédéral pour faire du Canada l'un des pays les plus branchés au monde. Le commerce électronique est un élément clé du programme. **(http://connect.gc.ca/fr/100-f.htm)**

[4] Dans le document « Connectedness Rankings », le Conference Board du Canada a placé le Canada derrière les États-Unis pour ce qui est de la connectivité globale (d'après un indice composé basé principalement sur des données de 1997-1998). Pour mieux comprendre ce que cela veut dire, disons que les données actuelles semblent indiquer que plus de la moitié des Canadiens sont branchés.

[5] *Pour une progression rapide : Comment faire du Canada un leader dans l'économie sur Internet.* La Table ronde sur les possibilités des affaires électroniques canadiennes a été établie par le Boston Consulting Group, avec l'aide d'Industrie Canada, en juin 1999. **(http://e-com.ic.gc.ca/equipe/)**

[6] Identificateur électronique joint à un document électronique. Semblable à une signature manuscrite. L'expression désigne presque toujours un identificateur généré au moyen de la cryptographie à clé publique (voir la prochaine section). L'expression *signature électronique* est utilisée dans un contexte plus vaste, pour indiquer qu'il s'agit de processus comportant des signatures numériques.

ii) ***l'intégrité*** - les données ne peuvent être modifiées sans que l'intervention ne soit décelée; et

iii) ***la non-répudiation*** - preuve qu'une communication a eu lieu ou qu'un message a été envoyé ou reçu (les parties ne peuvent donc pas nier que la communication a eu lieu).

Les techniques cryptographiques peuvent aussi assurer la ***confidentialité*** car elles permettent l'utilisation de technologies de chiffrement/déchiffrement pour rendre le texte original inintelligible et ainsi protéger l'information contre toute divulgation ou consultation non autorisée.

Ainsi, la cryptographie est un moyen important d'instaurer la confiance dans les marchés électroniques étant donné qu'elle permet à des parties qui ne se connaissent pas d'échanger et d'authentifier de l'information et de faire des affaires en toute sécurité dans un environnement en ligne. Les services liés à la cryptographie comportant des mécanismes d'authentification et de certification qui permettent cette fonctionnalité font partie intégrante des moyens visant à instaurer un climat de confiance.

d) Définition des services d'authentification et de certification

Même si on parle d'utilisation de processus d'authentification depuis des années dans l'environnement électronique (mots de passe, numéros d'identification personnelle ou « NIP », etc.), les techniques utilisées convenaient principalement à l'authentification des entités, pas à l'authentification des données ni des attributs. En outre, ces formes d'authentification ne confirment pas, en fait, l'identité de l'entité authentifiée, mais plutôt seulement le fait que l'entité participant à la transaction connaît le NIP, le mot de passe ou l'information personnelle (et, s'il y a lieu, qu'elle est en possession de la carte bancaire ou d'un jeton d'authentification). Échanger de l'information et conduire des affaires en ligne sur différents types de réseaux ouverts nécessite des méthodes d'authentification électronique et une gamme de services connexes d'appui.

On peut dire de l'authentification électronique qu'elle englobe toute méthode de vérification d'un élément d'information dans un environnement électronique, que ce soit l'identité de l'expéditeur d'un message (ou de l'auteur d'un texte), l'autorité d'une personne de participer à un genre particulier de transaction, les attributs de sécurité du matériel ou d'un logiciel, etc. Les techniques cryptographiques permettent d'exécuter cette fonction car elles font appel à des ***clés numériques***[7] pour chiffrer et déchiffrer des données numériques.

---

[7] Combinaison unique de un et de zéros.

Il existe deux grandes méthodes cryptographiques. En ***cryptographie à clé secrète***, la même clé sert à chiffrer et à déchiffrer les données. En ***cryptographie à clé publique***, il y a deux clés différentes, mais reliées l'une à l'autre, et ce qui est chiffré au moyen de l'une ne peut être déchiffré qu'au moyen de l'autre[8]. En plus de permettre le chiffrement à des fins de confidentialité, la cryptographie à clé publique permet d'authentifier ultérieurement des documents grâce à l'utilisation d'une clé privée qui crée une ***signature numérique***[9]. Cette technique assure aussi l'intégrité des documents et permet aux destinataires de déterminer si un message a été modifié d'une quelconque façon au cours de la transmission. C'est cette fonctionnalité qui présente un intérêt particulier pour le commerce électronique protégé sur des réseaux ouverts comme Internet.

La distribution honnête des clés publiques, combinée à des procédures visant à faire en sorte qu'une clé spécifique appartient réellement à un utilisateur donné, est essentielle à l'utilisation de la cryptographie à clé publique dans des réseaux ouverts. L'une des façons d'y parvenir est de faire appel à un tiers en qui l'on a confiance (ou une ***autorité de certification « AC »***[10]) pour gérer la distribution des clés publiques et des ***certificats***[11] contenant de telles clés. En plus de contenir la clé publique du détenteur de la clé, les certificats contiennent généralement de l'information au sujet du certificat comme tel, le nom de l'entité auquel le certificat a été délivré et des données au sujet du délivreur de certificat. Les données sont liées à l'entité, généralement par une signature numérique de l'AC.

Les certificats peuvent être délivrés pour une foule de raisons, qu'il s'agisse de fournir une assurance au sujet de l'identité ou encore de fournir plus de détails au sujet du détenteur du certificat en vue d'autoriser certaines interventions, comme celle d'effectuer des transactions. Les certificats peuvent aussi comporter divers niveaux d'assurance, ce qui indique le degré de confiance que l'on peut accorder à un certificat.

Pour qu'un certificat soit digne de confiance, il doit être délivré par une AC crédible, et les responsables des politiques d'intérêt public dans le monde s'efforcent actuellement de

---

[8] Une clé, connue comme étant la *clé publique*, est publiée dans ce que l'on peut considérer être l'équivalent d'un annuaire téléphonique. La *clé privée* connexe est gardée secrète.

[9] Identificateur qui est lié ou logiquement associé à un message ou à un document électronique. L'expéditeur « signe » un message avec la clé privée. L'expression « signature numérique » désigne presque toujours une signature électronique générale au moyen de la cryptographie à clé publique.

[10] Aux fins du présent document, l'expression « autorité de certification (AC) » est utilisée pour désigner un tiers en qui l'on a confiance, même s'il est reconnu qu'un tiers en qui l'on a confiance peut prendre différentes formes.

[11] Formulaire électronique qui ressemble à la version électronique d'un permis de conduire ou d'un passeport.

concevoir des moyens visant à faire en sorte qu'une AC et que les certificats qu'elle délivre soient dignes de confiance. Le commerce électronique planétaire a fait naître la nécessité d'avoir des démarches uniformes pour reconnaître le degré de confiance à accorder aux signatures numériques, la preuve de l'identité dans le cyberespace et la confiance mutuelle au sujet du niveau de confiance à accorder aux autorités de certification des divers secteurs de compétence.

Partie 1 - Contexte

1.1 Cadre politique actuel en vue d'instaurer la confiance

En 1996, en réponse aux recommandations du Comité consultatif sur l'autoroute de l'information, le ministre de l'Industrie a publié, au nom du gouvernement fédéral, un rapport exhaustif qui indiquait en détail les mesures à prendre pour créer une société du savoir[12]. En ce qui concerne le commerce électronique, le rapport mentionnait la nécessité de protéger les transactions électroniques.

En travaillant en étroite collaboration avec le secteur privé, le gouvernement fédéral a précisément répondu à ce besoin, ainsi qu'à l'exigence connexe qui consiste à instaurer un climat de confiance à l'égard du commerce électronique en général, en mettant en place des initiatives stratégiques dans les secteurs suivants.

a) Protection des consommateurs

Des représentants de l'industrie, du gouvernement et des consommateurs ont conjointement élaboré un ensemble de principes et de lignes directrices pour la protection des consommateurs faisant des affaires en ligne[13]. Les principes visent à orienter les actions des entreprises, des consommateurs et des gouvernements canadiens dans la mise en place d'un cadre pour protéger les consommateurs relativement au commerce électronique sur des réseaux ouverts, dont Internet. Les principes reconnaissent qu'un cadre solide visant à protéger les consommateurs favorisera la confiance de la clientèle et facilitera l'acceptation et la croissance du commerce électronique. Le Bureau de la consommation (BC) d'Industrie Canada collabore actuellement avec le secteur privé et ses homologues provinciaux pour « opérationnaliser » ces principes.

b) Protection des renseignements personnels

La *Loi sur la protection des renseignements personnels et les documents électroniques* a

---

[12] *La société canadienne à l'ère de l'information : Pour entrer de plain-pied dans le XXIe siècle* (mai 1996).

[13] *Principes régissant la protection des consommateurs dans le commerce électronique : Le cadre canadien* (novembre 1999). Définis par le Groupe de travail sur la consommation et le commerce électronique (coordonné par le Bureau de la consommation d'Industrie Canada). Voir **http://strategis.ic.gc.ca/SSGF/ca01180f.html** pour obtenir la liste des principes et plus d'information sur ce travail.

été adoptée par le Parlement en avril 2000[14]. Les dispositions de la partie 1 de la Loi établissent les règles qui gouverneront la collecte, l'usage et la communication des renseignements personnels. Elles entreront en vigueur le 1er janvier 2001. Ces dispositions sur la protection des renseignements personnels contribueront à instaurer la confiance à l'égard du commerce électronique en prévoyant des assurances de protection concernant les renseignements personnels sous forme numérique. Elles uniformisent les règles du jeu pour le commerce en établissant des règles claires et prévisibles pour tous. Les consommateurs et les entreprises seront en mesure de mener leurs transactions en ligne en étant confiants que les mesures de protection des renseignements personnels sont en place et que le Commissaire à la protection de la vie privée se charge de les faire respecter.

c) Cadre juridique

La nouvelle *Loi sur la protection des renseignements personnels et les documents électroniques* crée également un moyen électronique de faire des affaires avec le gouvernement fédéral.[15] Les dispositions pertinentes, qui correspondent aux parties 2 à 4 de la Loi, visent les points suivants :

i) Signature électronique sécurisée

La Loi a établi que les ministères, organismes et conseils fédéraux auront le pouvoir de décider de quelle façon les exigences des lois et règlements existants peuvent être remplies par voie électronique. Ces dispositions sont entrées en vigueur le 1er mai 2000. Une composante clé de la législation est le concept de la ***signature électronique sécurisée***[16], qui peut être utilisée dans les transmissions électroniques.

ii) Gouvernement en ligne

La nouvelle législation procure au gouvernement fédéral un moyen de mener des affaires par voie électronique. Ce qui est maintenant possible sur papier le sera par voie électronique. La Loi donne aux moyens électroniques une valeur équivalente au format papier.

---

[14] Ancien projet de loi C-6. Pour plus d'information, voir (**http://e-com.ic.gc.ca/francais/privee/632d1.html**).

[15] Pour plus d'information sur ces dispositions de la Loi, voir (**http://e-com.ic.gc.ca/francais/fastfacts/43d9.html** et **http://canada.justice.gc.ca/fr/ps/ce/index.html**).

[16] Définie comme étant une « Signature électronique qui résulte de l'application de toute technologie ou de tout procédé par règlements [...] ». Ces règlements sont élaborés par le Conseil du Trésor.

iii) Preuve électronique

La nouvelle législation précise comment les tribunaux évaluent la fiabilité d'un document électronique qui est présenté en preuve, approuvent les règlements pour aider les tribunaux à associer les signatures électroniques sécurisées auxpersonnes, et reconnaissent que les avis et les lois publiés électroniquement par l'imprimeur de la Reine ont le même statut légal que ceux publiés sur papier par l'imprimeur de la Reine.

d) Sécurité

En octobre 1998, le gouvernement fédéral a publié sa politique en matière de cryptographie qui comprend des dispositions sur l'utilisation de la cryptographie dans la conduite du commerce électronique[17]. La politique répond à la nécessité de protéger certaines catégories de transactions électroniques en faisant en sorte que les Canadiens puissent mettre au point, importer et utiliser les produits qu'ils veulent en matière de cryptographie. Elle envisage des cas où les techniques cryptographiques permettent d'établir l'identité et les privilèges des parties aux transactions, souvent grâce à des tiers en qui l'on a confiance, comme les AC. La politique rejette l'idée d'obliger les autorités de certification à obtenir un permis en faveur d'une accréditation des autorités de certification du secteur privé dirigée par l'industrie.

---

[17] Voir **http://e-com.ic.gc.ca/francais/crypto/631d1.html** pour obtenir plus d'information sur la politique en matière de cryptographie.

Partie 2 - Définition d'un programme pour l'avenir

2.1 Constatations des intervenants

a) Nécessité de définir un cadre

Même si les intervenants sont d'avis que la concurrence et l'innovation sont des objectifs importants dans le marché émergent, ils reconnaissent également que les nouveaux marchés se développent mieux quand les utilisateurs ont confiance dans les produits et services qu'ils reçoivent. Les intervenants reconnaissent que la nécessité d'instaurer la confiance est aussi importante que le besoin de promouvoir la concurrence. Or, il peut se révéler difficile d'en arriver à un équilibre approprié et efficace qui réponde aux besoins de tous les intervenants, qu'ils soient fournisseurs, utilisateurs ou autres.

La majorité des intervenants ont aussi remarqué qu'il existe des coûts d'efficience du marché et des questions de confiance du public qui sont associés à une approche de laissez-faire relativement à ce nouveau marché. Ils craignent que les coûts et les risques soient importants pour toutes les parties étant donné que de nouveaux processus opérationnels sont élaborés et mis en oeuvre. Certains estiment que la confiance doit être considérée comme un bien public qui ne peut être garanti par les seules forces du marché.

Jusqu'à maintenant, les consultations ont mis au jour quatre raisons pour lesquelles il serait souhaitable d'établir un cadre pour les services d'authentification et de certification.

- Procurer aux utilisateurs un moyen d'établir la fiabilité des autorités de certification.
- Établir des régimes d'authentification offrant un niveau de confiance uniforme et vérifiable.
- Permettre aux utilisateurs de faire des choix à partir de paramètres connus pour la confiance.
- Réduire au minimum les situations où les entreprises et consommateurs participant à plus d'un régime d'authentification pourraient avoir à respecter des exigences différentes (voire conflictuelles).

b) Compatibilité nationale

Les intervenants ont également signalé qu'un cadre pour les services d'authentification et de certification facilitera l'adoption de pratiques juridiques et techniques solides et

cohérentes par les autorités de certification au Canada. Une certaine uniformité rendra aussi compatibles les approches des divers secteurs de l'industrie, compatibilité à laquelle s'attendront vraisemblablement les utilisateurs à l'échelle nationale[18].

Ils ont aussi insisté sur le fait qu'il faut que les provinces aient des approches compatibles, ce qui permettra d'éviter les obstacles et de prévoir l'interopérabilité nécessaire au commerce électronique national. Les intervenants sont d'avis que la coordination fédérale-provinciale est nécessaire et souhaitable pour réaliser cet objectif; c'est pourquoi ils ont laissé entendre que des tables rondes existantes pourraient servir à cette fin. En ce qui concerne le secteur public, on envisage le Conseil des DPI du secteur public[19] comme moyen efficace potentiel de coordination. Pour ce qui est des tables rondes des secteurs public et privé, la Conférence pour l'harmonisation des lois au Canada (CHLC)[20] pourrait jouer le même rôle. La CHLC a déjà élaboré la Loi uniforme sur le commerce électronique[21] qui représente une initiative importante visant à assurer un fondement à la coordination des cadres juridiques provinciaux.

c) Compatibilité internationale

D'un point de vue international, un cadre peut aider considérablement à faciliter la reconnaissance des certificats canadiens à l'échelle internationale. La compatibilité internationale est importante sur deux plans. Tout d'abord, il est essentiel d'avoir une acceptation et une utilisation globales des services canadiens. Ensuite, il faut s'assurer que le Canada remplisse ses obligations liées au commerce international. Tout manquement aux normes internationales pourrait restreindre le commerce du Canada avec d'autres pays et donner lieu à des blocages transfrontaliers.

Les approches adoptées par les diverses instances varient. Ce sera donc un défi que d'élaborer un cadre qui facilitera la reconnaissance des certificats canadiens. Il faut prendre des mesures pour que les certificats délivrés par les organisations canadiennes soient acceptables dans les provinces qui administrent une gamme de régimes différents qui vont des AC réglementées ou avec permis aux AC non réglementées. D'un point de vue canadien, où l'obtention d'un permis n'est pas une exigence du gouvernement fédéral, il sera vraisemblablement plus facile de relever les défis liés à l'élaboration d'une approche canadienne pour les discussions internationales soit si les AC ne sont pas contrôlées, soit si une approche d'accréditation dirigée par l'industrie peut

---

[18] L'ampleur et la portée de la compatibilité ou de l'interopérabilité nécessaire ou souhaitable variera. Par exemple, sa portée pourrait se limiter à un secteur d'activité, s'étendre à plusieurs d'entre eux ou simplement entrer en ligne de compte en aval ou en amont de la chaîne d'approvisionnement.

[19] Le Conseil des DPI du secteur public est composé des dirigeants principaux de l'information (DPI) du Canada, c'est-à-dire des provinces, des territoires et du gouvernement fédéral. **(http://www.tbs-sct.gc.ca/cio-dpi/psciоc/psciоc_home_f.html)**

[20] Organisation indépendante constituée de représentants de la magistrature, des ministères de la justice, des facultés de droit, des praticiens de la profession.

[21] Septembre 1999. **(http://www.law.ualberta.ca/alri/ulc/current/fueca.htm)**

être adoptée rapidement. [22] On pourrait devoir faire face à des défis de taille dans les provinces où les services des AC sont réglementés, en particulier là où on recherche la reconnaissance transfrontalière (ou la certification transfrontalière). Il semble qu'il n'y ait actuellement aucun obstacle de cette nature au sein de l'environnement nord-américain. Cependant, il est déjà évident que des obstacles risquent d'exister en Europe et en Asie, et il faudra donc se pencher sur les diverses façons de les surmonter[23].

La participation soutenue du Canada à diverses tribunes internationales où il est question du besoin de cadres mondiaux applicables à l'authentification constitue donc une dimension permanente indispensable. Le Canada concentre actuellement ses démarches internationales auprès de la Commission des Nations Unies pour le droit commercial international (CNUDCI) pour ce qui est des questions juridiques, et auprès de l'Organisation de coopération et de développement économique (OCDE) et de la Coopération économique Asie-Pacifique (APEC), pour ce qui est des discussions relatives aux politiques publiques[24]. Il est entendu qu'une étroite collaboration entre le gouvernement fédéral et le secteur privé est un élément essentiel de cette participation. Les intervenants laissent également entendre que le Canada pourrait compléter cette participation par des consultations bilatérales ou multilatérales visant à élaborer des protocoles d'entente ou des déclarations conjointes avec d'autres pays et d'autres instances[25].

---

[22] Annonce faite par le ministre de l'Industrie en octobre 1998 dans le contexte de la politique en matière de cryptographie. Toutefois, même si le gouvernement fédéral a indiqué qu'il n'imposerait pas un régime de délivrance de permis, les provinces n'ont pas encore fait de même. Aussi, il est théoriquement possible que le Canada se retrouve avec un mélange d'AC détentrices et non détentrices de permis si au moins un gouvernement provincial décide d'obliger les AC oeuvrant sur son territoire à obtenir des permis.

[23] Il pourrait être difficile pour les AC étrangères de se conformer aux exigences des lois de l'Italie ou de l'Allemagne. Cette question fait l'objet de discussions permanentes dans les forums internationaux. Un projet qui peut être particulièrement utile pour cerner les obstacles potentiels à l'authentification transfrontalière est une initiative actuelle mise de l'avant par un groupe d'étude d'experts du Groupe de travail de l'APEC sur les télécommunications. Le projet porte sur l'établissement de processus clés en vue d'instaurer la confiance à l'égard de la certification et sur l'organisation de régimes existants en fonction de ces éléments clés. Ce projet facilitera la concertation des différentes approches et offrira une analyse sur l'adaptation des variantes afin de répondre aux mêmes objectifs.

[24] Le ministère de la Justice est chargé d'élaborer les positions canadiennes pour les travaux au sein de la CNUDCI. Des représentants de la Direction du commerce électronique participent aux comités et aux groupes de travail pertinents de l'OCDE/APEC.

[25] Pour le moment, le Canada est signataire de déclarations conjointes avec l'Australie et l'Union européenne. Même si ces déclarations s'appliquent au commerce électronique en général, il est possible que d'autres consultations et négociations soient entreprises et qu'elles portent plus précisément sur les aspects de l'authentification avec les plus importants partenaires commerciaux du Canada. (**http://e-com.ic.gc.ca/francais/releases/41d12.html**) et (**http://ecom.ic.gc.ca/francais/71ta.html**)

La discussion sur la comptabilité à l'échelle internationale fait ressortir le rôle important et continu que les gouvernements ont à jouer à titre « d'instigateurs d'un climat de confiance » dans cet environnement. Or, la nécessité pour les entreprises d'établir des relations de confiance à l'échelle internationale semble indiquer que les gouvernements continueront à jouer un rôle important puisque la multitude d'initiatives actuelles du secteur privé visant l'élaboration de cadres mondiaux pourrait nécessiter une forme quelconque d'appui gouvernemental, spécialement les initiatives intersectorielles. Bon nombre de ces initiatives menées par le secteur privé (par exemple, les comités pertinents relevant de l'American Bar Association, la nouvelle table ronde sur l'ICP[26], etc.) prévoient déjà la participation de représentants du gouvernement.

d) Dimensions liées à la concurrence

Des intervenants ont fait remarquer que, le marché des services d'authentification et de certification venant à peine d'éclore, le nombre de fournisseurs est restreint et la concurrence est limitée. Ils ont constaté que le marché offre de nouveaux débouchés pour certains secteurs d'activité, en mettant à la disposition de ceux qui ne prenaient pas déjà part, dans une certaine mesure, au commerce électronique, la technologie qui leur permet d'offrir de nouveaux services et d'assumer de nouveaux rôles. Des intervenants se sont dits préoccupés par le fait que des solutions liées au marché uniquement n'aboutiront pas nécessairement à des règles équitables pour tous les intervenants. Par exemple, il se peut que les règles du jeu ne soient pas équitables d'où les entités réglementées entrent en concurrence avec les entités non visées par une surveillance réglementaire, Si c'était le cas, cette situation pourrait avoir des répercussions sur les utilisateurs finaux puisque le degré de protection offert aux consommateurs pourrait varier. Si la complexité de la technologie et des services fournis ne permet pas aux utilisateurs de faire une distinction entre les AC, il pourrait en découler de la confusion, des coûts cachés et une augmentation des risques (inconnus), ce qui entraînerait de la frustration chez les utilisateurs. La mise en place d'un cadre pour l'authentification au Canada peut contribuer à rendre les règles équitables pour tous les joueurs.

L'élaboration d'un cadre aidera également les consommateurs à faire des choix importants. Dans un marché concurrentiel, les consommateurs sélectionneront, en règle générale, les AC en fonction de la performance et du coût qui, dans la plupart des cas, sera indiqué dans le contrat. Par ailleurs, compte tenu de l'ensemble des questions techniques, opérationnelles ou juridiques liées à la prestation de services des AC, des contrats afférents pourraient être longs et complexes. Cela constituerait un fardeau déraisonnable pour le consommateur qui devrait alors être en mesure d'analyser ces contrats, d'établir des distinctions pertinentes entre les AC et de faire des choix rationnels. Cela serait d'autant plus difficile que le consommateur pourrait devoir

---

[26]Initiative de collaboration dirigée par l'industrie qui a été mise sur pied pour accélérer l'adoption de la technologie de l'infrastructure à clé publique et de solutions axées sur l'ICP, comme la fondation sûre pour les applications des affaires électroniques protégées. (**http://www.pkiforum.org**)

consulter d'autres documents très longs comme la politique de certification[27] et l'énoncé de pratiques de certification[28] afin de comprendre, par exemple, l'approche des AC relativement à la reconnaissance mutuelle ou l'intercertification. Un cadre applicable à cette relation contribuerait à promouvoir la libre et loyale concurrence et ferait en sorte qu'elle soit fondée sur l'objectivité.

e) Aspects liés au développement des marchés

En offrant une coordination en vue du développement et de l'utilisation de services d'authentification électroniques, on contribuera aussi à la création d'un environnement propice au renforcement de la position concurrentielle des grandes et des petites entreprises sur le marché. Le Canada est déjà un joueur important dans les segments de marché du commerce électronique liés aux produits et services de sécurité. Par ailleurs, en assurant la coordination en vue du développement et de l'utilisation de ces services et la promotion de leur utilisation à grande échelle dans tous les secteurs, on permettra au Canada de tirer profit des possibilités et des avantages qui se présentent au niveau de l'emploi et de la croissance.

2.2 Portée proposée du cadre

Le cadre devra tenir compte des composantes suivantes du commerce électronique : entreprise-entreprise et entreprise-consommateur. Les composantes entreprise-gouvernement et gouvernement-entreprise relèvent du Secrétariat du Conseil du Trésor dans le contexte de son rôle dans la conception, l'élaboration et la coordination de l'infrastructure à clé publique du gouvernement du Canada[29] (ainsi que d'autres ministères qui optent pour d'autres approches en vue de répondre à des exigences précises). De même, les composantes particulier-gouvernement et gouvernement-particulier[30] n'entrent pas dans la portée de la stratégie. On reconnaît toutefois que les démarches mises en oeuvre dans le secteur public et que la composante gouvernement-entreprise auront une influence.

---

[27] Une politique de certification indique l'applicabilité d'un certificat à une collectivité ou à une classe d'application particulière. Elle définit également les parties, leurs relations et leurs obligations.

[28] L'énoncé de pratiques de certification fait état des procédures dont une AC se sert pour délivrer et gérer les certificats. On peut dire de la politique de certification qu'elle correspond au « quoi » et de l'énoncé de pratiques de certification qu'il correspond au « comment ».

[29] Communément connue sous le nom de « ICP-GC ». L'ICP-GC assurera un processus uniforme de gestion et de certification des clés à l'échelle du gouvernement. **(http://www.cio-dpi.gc.ca/pki/Initiatives/initiatives_f.html)**

[30] Désigné sous le nom de « Gouvernement en ligne » ou « GEL ». Le projet vise à fournir aux Canadiens un accès à l'information et aux services gouvernementaux en ligne.

Le cadre aura pour objet d'orienter le développement et l'utilisation des services d'authentification au Canada. Toutefois, pour ce faire, la stratégie devra reconnaître et appuyer les avantages liés au choix et à la liberté de contrat en permettant aux parties de déterminer les modalités qui conviennent le mieux à leurs transactions ou à leurs communications. À cet égard, la stratégie ne chercherait pas à exclure ou à entraver les approches basées sur les contrats, mais plutôt à fournir une certaine communauté d'éléments, prévisibilité et confiance aux utilisateurs des services.

Finalement le cadre devra idéalement être neutre sur le plan de la technologie et de l'architecture. Toutefois, compte tenu du fait que ce sont surtout les infrastructures à clé publique qui permettent de répondre aux exigences du commerce électronique en matière de sécurité, il se pourrait que l'on ait à axer des aspects sur les infrastructures à clé publique pour que la stratégie ait un sens dans la réalité de l'environnement actuel et pour qu'elle s'y applique[31]. Ce faisant, il ne faudrait toutefois pas chercher à empêcher l'utilisation d'autres technologies ni l'examen de cette stratégie à la lumière des nouvelles percées technologiques.

[31] Même si un des objectifs de ce travail consiste à rester neutre sur le plan de la technologie, cela s'est déjà avéré problématique lors de certains forums. Par exemple, même si la CNUDCI a adopté au départ une approche neutre sur le plan de la technologie afin de préparer des règles qui prévoient plus de certitude si on se sert d'une technologie particulièrement fiable pour la signature, les travaux sont maintenant concentrés sur les signatures numériques (créées avec une cryptographie à clé publique) puisque c'est la méthode la plus connue pour le moment.

Partie 3 - Un cadre pour les services d'authentification et de certification - Approche proposée

3.1 Généralités

Jusqu'à maintenant, les consultations ont permis de démontrer que les intervenants sont intéressés à établir une approche concertée pour instaurer la confiance. Même s'ils ne se sont pas encore penchés sur la nature et la portée précises de cette approche concertée, quelle qu'elle soit, la plupart se sont entendus sur l'utilité d'avoir une certaine forme de principes communs fondés sur le marché pour orienter le développement et l'utilisation des services d'authentification au Canada. Il sont surtout d'avis que ces principes devraient être de nature générale et intersectorielle de manière à fournir un niveau de clarté et d'uniformité aux utilisateurs finaux, à améliorer les possibilités d'interopérabilité et à bien positionner le Canada à l'échelle internationale. On remarque que de tels principes pourraient, à leur tour, servir de fondement à l'accréditation des autorités de certification[32]. C'est pourquoi la portée et le contenu de ces principes méritent qu'on s'y attarde. Il faut étudier des modèles et des critères d'accréditation potentiels pour cerner ces aspects (p. ex., les responsabilités des divers joueurs, etc.) qui devront être pris en considération dans l'élaboration des principes.

3.2 Principes

a) Généralités

Il existe de nombreux exemples de principes directeurs qui ont été élaborés par divers forums internationaux. Les *International Consensus Principles for Electronic Authentication,* élaborés par le *Internet Law and Policy Forum* (ILPF)[33], pourraient servir de modèles à l'élaboration de principes au Canada. En outre, le travail accompli par les groupes *Alliance of Global Business* (AGB) et *Global Business Dialogue* (GBDe) est un bon exemple des objectifs et des attentes du secteur privé, dont on devrait s'inspirer pour veiller à ce que l'approche du Canada soit compatible avec les orientations internationales.

---

[32] L'accréditation renvoie au processus d'évaluation et de certification concernant la véracité des services d'authentification et de certification. Il est en général reconnu que, dans cet environnement, l'accréditation des autorités de certification constitue un élément essentiel à n'importe quel cadre des services d'authentification. Dans cette optique, le concept d'accréditation a été intégré au travail de plusieurs grands forums internationaux et de l'industrie.

[33] Il s'agit d'une table ronde non gouvernementale favorisant le dialogue et l'échange d'information informels relativement à toute question juridique ou d'orientation concernant le réseau Internet et le commerce électronique. Les principes (avril 1999) visent à faciliter le commerce électronique mondial à partir de la création d'un environnement juridique prévisible concernant l'authentification électronique qui protège les utilisateurs et reflète leurs besoins. (**http://ilpf.org**)

Fondamentalement, ces organismes préconisent dans tous les cas que les approches nationales respectent la liberté contractuelle et recherchent des solutions neutres sur le plan de la technologie ou de l'architecture informatique et qui sont déterminées par le marché. Ces objectifs sont conformes à ceux qu'Industrie Canada a fixés en consultation avec les intervenants.

En outre, certains secteurs industriels particuliers ont également entrepris des initiatives dans ce domaine qui serviront de modèles à l'élaboration des principes. Les *Lignes directrices CARAT* [34] (une publication de la « NACHA » - la National Clearing House Association) peuvent servir de point de départ aux discussions sur les attentes de nature commerciale et juridique ainsi que sur les relations et les exigences des diverses parties en cause. Ces *Lignes directrices* peuvent être particulièrement utiles étant donné qu'elles sont souples et génériques et qu'elles se prêtent à une application à une vaste gamme de modèles d'entreprises. Les *American Bar Association Guidelines*[35] peuvent aussi être utiles étant donné qu'elles fournissent un cadre pour les discussions sur les aspects juridiques.

Les travaux de l'Institut canadien des comptables agréés (ICCA) et de l'American Institute of Certified Public Accountants (AICPA) relativement aux services Webtrust sont également intéressants[36]. Les programmes de sceaux existants ou émergents sur le Web peuvent aussi avoir une incidence sur les principes[37].

Comment les travaux en cours et les documents existants peuvent-ils être adaptés à l'élaboration de principes au Canada?

---

[34] Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates. Élaborées sous les auspices du Internet Council, un conseil parrainé par la NACHA. Elles se trouvent à l'adresse suivante : **(http://internetcouncil.nacha.org)**.

[35] *« Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce »* (août 1996). American Bar Association Information Security Committee. **(http://www.abanet.org/scitech/scitechpubs.html)**

[36] *Principes et critères WebTrust pour le commerce électronique entre entreprises et consommateurs* (octobre 1999). Accessibles à : **(http://www.cica.ca/cica/cicawebsite.nsf/public/Aproposdeswebtrust)**. *« WebTrust Principles and Criteria for Certification Authorities »* **http://WWW.AICPA.ORG/homepage.htm**

[37] L'idée de l'adoption d'une « marque de confiance » canadienne proposée par les participants à la Table ronde sur les possibilités des affaires électroniques canadiennes est particulièrement intéressante. Ce concept est étudié par l'une des six équipes qui effectuent le suivi sur les recommandations découlant de la Table ronde (en collaboration avec le Bureau de la consommation).

b) Applicabilité et portée

En règle générale, la documentation actuelle et les discussions stratégiques sur les tribunes internationales classent les modèles d'authentification selon qu'il existe un lien de droit contractuel entre les parties. Plus précisément, on reconnaît généralement que dans les cas où il existe un lien de droit contractuel entre les parties, il s'agit d'un « modèle fermé ». Ce modèle contraste avec les « modèles ouverts », où l'on retrouve des relations indirectes. Entre les deux, il existe une foule de modèles « hybrides » ou « ouverts mais liés ». L'introduction d'intermédiaires dans les divers modèles et la nature changeante des relations possibles (p. ex., relation d'agence ou simple rôle de point de transit, etc.) multiplie encore les variantes possibles.

Des intervenants sont d'avis qu'il faudra faire face à des questions juridiques dans cet environnement, même si on se fie aux contrats et que dans ce cas, il serait utile que les modèles ouverts et fermés aient des paramètres communs. D'autres sont allés plus loin et fait remarquer qu'en raison de la complexité des contrats qui seront probablement exigés dans cet environnement, comprendre les contrats et faire des choix et des comparaisons éclairés constitueront peut-être un fardeau trop lourd pour les consommateurs. En se basant sur cela, il sera nécessaire d'appliquer un ensemble de principes communs à tous les modèles. Toutefois, on a laissé entendre que, dans certains cas, les détails de leur mise en oeuvre peuvent varier, particulièrement dans le cas des modèles fermés.

Par exemple, la responsabilité et les aspects qui y sont associés peuvent constituer des secteurs où l'applicabilité des principes peut différer dans les modèles fermés à cause d'au moins deux raisons. Tout d'abord, on a donné à penser que les modèles fermés devraient être considérés dans le contexte du modèle commercial général, où les risques sont répartis sur l'ensemble de l'infrastructure et atténués par un certain nombre de composantes. Ensuite, on a laissé entendre que les modèles fermés pourraient répartir les risques plus efficacement, étant donné qu'ils permettront généralement de contrôler tous les aspects du processus d'authentification. Il a donc été soutenu que l'ensemble du modèle commercial et les attributs de sécurité qui y sont incorporés doivent être évalués au moment de déterminer l'applicabilité des principes. Cela ne signifie pas que seuls certains principes seraient pertinents dans ces circonstances, mais plutôt que les détails de mise en oeuvre de chacun d'eux peuvent varier. En raison de la très grande complexité des questions qui seront réglées par ces principes, il ne serait pas indiqué d'en choisir uniquement un sous-ensemble.

De plus, on reconnaît que les modèles différeront non seulement par le fait qu'ils offrent des services aux collectivités ouvertes ou fermées, mais également par le niveau de confiance et d'assurance qu'ils offrent. Ce sont donc les applications individuelles qui

détermineront les niveaux appropriés de confiance et d'assurance offerts par les AC. Les AC varieront également de par leur structure, ce qu'il faudra prendre en compte[38]. Toutefois, peu importe l'éventail de modèles et la mise en oeuvre particulière, on peut présumer que toutes auront certains processus fondamentaux communs et certaines exigences de régie. Ce sont au moins ces aspects qu'il faudra traiter en commun au niveau des principes si l'on veut en arriver à un cadre logique pour les services d'authentification.

Dans quelle mesure les principes devraient-ils influer sur les modalités des contrats qui régiront les services relatifs à l'authentification dans des environnements fermés? Dans quelles circonstances conviendrait-il de varier les aspects de mise en oeuvre des principes?

c) Teneur

Les intervenants qui ont participé jusqu'à maintenant au programme de consultation ont formulé des commentaires concernant plusieurs secteurs dont on devra tenir compte dans l'élaboration des principes. Voici les aspects qui ont été mentionnés par pratiquement tous les intervenants consultés jusqu'à maintenant :

i) Protection des renseignements personnels

Les intervenants sont d'avis que tout principe élaboré devra établir certains paramètres visant à assurer que les services d'authentification et de certification ***respectent la protection des renseignements personnels***. Même si les dispositions sur la protection des renseignements personnels de la nouvelle législation (la *Loi sur la protection des renseignements personnels et les documents électroniques*) s'appliqueront aux AC elles-mêmes, il faudra veiller à ce que les processus dérivés ou secondaires associés aux services qu'elles offrent respectent également la protection des renseignements personnels.

ii) Divulgation

Quasiment tous les intervenants consultés jusqu'à présent ont convenu de la nécessité de la pleine ***divulgation*** des droits et responsabilités de toutes les parties en cause. De la même façon, la divulgation intégrale à toutes les personnes concernées (utilisateurs, fournisseurs, tierces parties et parties intéressées) des risques et des responsabilités d'une opération sera vraisemblablement un élément

[38] Certains modèles comporteront des relations hiérarchiques entre une AC principale et une foule d'AC subordonnées. D'autres modèles comporteront des relations qui jettent des « ponts » entre diverses AC.

important des principes. Cela sera particulièrement crucial dans le contexte des applications et des mises en oeuvre dotées de la fonction de non-répudiation[39].

iii) Responsabilité

La question de l'incertitude entourant la responsabilité a été soulevée à plusieurs reprises par les intervenants. À leur avis, on devrait peut-être élaborer des ***lignes directrices sur la responsabilité*** relativement à ces services. Plus précisément, la majorité d'entre eux pensent qu'on devrait traiter de manière générale, au niveau des principes, la mesure à laquelle les AC peuvent limiter leur responsabilité ou y échapper pour des pertes découlant de l'utilisation de leurs certificats par des parties fiables. Certains pensent même que le niveau minimal de responsabilité de la part des AC devrait être précisé, et leur immunité définie d'une façon ou d'une autre[40].

Sur quels autres domaines les principes devraient-ils porter? Et pourquoi?

d) Respect

Même s'il est clair que les principes seraient non exécutoires et volontaires, la plupart des intervenants ont laissé entendre qu'une certaine forme de mécanismes de respect sera nécessaire. Toutefois, on s'interroge sur la forme qu'ils devraient prendre et il se pourrait bien qu'une foule d'approches soient appropriées, selon la nature du service offert par l'AC et selon que l'on a recours à des modèles ouverts ou fermés.

Certains groupes d'intervenants soutiennent que la seule approche efficace serait d'exiger des examens par des organismes indépendants et laissent entendre que les entités de vérification existantes pourraient être bien placées pour l'appliquer à cet environnement[41]. D'autres

---

[39] Les taux élevés de rejets des opérations effectuées avec une carte de crédit sur le réseau Internet laissent supposer que les consommateurs devront être parfaitement renseignés sur les mises en oeuvre dotées de la fonction de non-répudiation qui n'offrent pas de souplesse.

[40] D'autres dimensions pourraient être ajoutées à cette discussion si l'on déterminait que des « secteurs » de responsabilité de base doivent être établis vu qu'il faudrait probablement s'organiser pour qu'ils soient différents selon que des transactions entreprise-entreprise ou entreprise-consommateur sont en cause.

[41] Des initiatives de l'industrie sont déjà en cours à cet égard. Par exemple, l'American Institute of Chartered Accountants et l'Institut Canadien des Comptables Agréés ont préparé un exposé-sondage intitulé « *WebTrust Principles and Criteria for Certification Authorities* » qui constitue un cadre d'évaluation de la pertinence et de l'efficacité des contrôles employés par les AC. **(http://www.AICPA.ORG/homepage.htm)**

estiment que toute exigence d'examens indépendants peut constituer un obstacle sur le plan des coûts [42] et considèrent une approche d'autoréglementation par l'industrie comme étant souhaitable. Une telle approche pourrait comporter des autodéclarations de conformité aux principes et pourrait peut-être être étayée par des pénalités et des dommages pour non-respect. L'adoption d'une telle approche aurait des répercussions sur les autres éléments de l'approche (p. ex. il serait nécessaire de divulguer pleinement l'information).

Les assurances nécessaires au sujet des acteurs pourraient être obtenues grâce à l'établissement d'une série d'autorités de « haut niveau » (p. ex. les entités dignes de confiance déjà existantes ou les entités réglementées pourraient être établies comme AC) et découler de la certification croisée (ou d'accords de reconnaissance mutuelle) avec ces autorités de haut niveau. Toutefois, il faudrait examiner les dimensions concurrentielles de l'adoption de cette solution particulière.

Ceux qui ne croient pas à la nécessité d'une composante conformité ont laissé entendre que l'utilisation dans le marché devrait agir comme contrôle, supposant que les mécanismes inadéquats ou inférieurs ne survivront tout simplement pas. Toutefois, dans cette approche, on suppose un certain niveau de compréhension de la technologie de la part des utilisateurs qui n'existe peut-être pas encore.

Comment traiter la question du respect? Dans quelles circonstances est-il souhaitable d'avoir une certaine forme d'évaluation ou de vérification des principes? Qui devrait assurer la fonction d'évaluation? En fonction de quels critères? Que se passe-t-il si l'on fait reposer la conformité sur les autodéclarations? Dans quelles circonstances conviendrait-il de dériver les assurances nécessaires des relations avec les entités existantes dignes de confiance?

e) Rôle des AC du secteur public (en particulier l'ICP-GC)

Dans le contexte de l'engagement qu'il a pris d'utiliser les technologies de l'information pour offrir des services novateurs aux Canadiens et pour améliorer l'efficacité des opérations gouvernementales, le gouvernement du Canada (GC) a mis en oeuvre une architecture de sécurité de portée générale pour la prestation de services par voie électronique. Une infrastructure à clé publique (ICP) a été mise au point pour assurer la confidentialité, l'intégrité des données, l'authentification et la non-répudiation, éléments qui sont nécessaires pour assurer une meilleure protection de la vie privée et pour protéger les transactions électroniques. Cette

[42] Les intervenants ont toutefois laissé entendre que les consommateurs pourraient considérer un obstacle de cette nature comme salutaire, en ce sens qu'il réduirait la possibilité que les AC offrent des services « malhonnêtes ».

infrastructure apporte la sécurité et la confiance nécessaires pour la conduite des affaires électroniques du gouvernement.

Dans la mesure où les affaires du gouvernement exigent une interaction avec le secteur privé et dans la mesure où la demande d'accès aux services électroniques du gouvernement peut faire naître le besoin de fournisseurs de services d'authentification dans le secteur privé, le rapport entre l'ICP-GC et le présent travail doit être gardé en mémoire. En particulier, la méthodologie et les critères de cocertification[43] qui ont été élaborés pour les AC qui souhaitent « interagir » avec l'ICP-GC pourraient avoir un rôle à jouer dans l'élaboration des principes (particulièrement dans le contexte des principes sur lesquels reposera l'accréditation des AC du secteur privé)[44]. Les critères et les procédures de l'ICP-GC peuvent aussi être importants dans le sens où les ICP provinciales pourraient les suivre dans l'avenir.

f) Mécanisme d'élaboration des principes

Pour élaborer les principes, on pourrait envisager de faire appel à une association existante dont on élargirait la représentation (pour les besoins de la cause) qui s'étendrait à d'autres secteurs industriels et à des gouvernements. On pourrait aussi décider de créer un nouveau forum expressément pour traiter cet aspect (et peut-être d'autres aspects) de l'authentification[45].

Quelle que soit la nature précise du forum choisi, l'élaboration des principes devra être fondée sur la participation et la collaboration d'un grand nombre d'intervenants si l'on veut tenir compte des intérêts et des besoins de tous les groupes. On devra accepter le défi d'en arriver à un équilibre entre les intérêts de ces groupes et de gérer les aspects concurrentiels (voir partie 4.1c). Étant donné que les intervenants sont d'avis que la collaboration entre les secteurs public et privé est indispensable à la réalisation de la majeure partie du programme prévu pour l'avenir, il est souhaitable que le secteur public intervienne pour assurer l'équilibre et la neutralité du processus.

---

[43] *Infrastructure à clé publique du gouvernement du Canada : Méthodologie et critères de cocertification* (septembre 1999). Voir (**http://www.cio-dpi.gc.ca/pki/Documents/documents_f.html**).

[44] Les relations avec les AC du secteur public pourraient offrir au secteur privé des solutions de rechange qui leur permettraient de se faire accréditer dans le cadre de régimes dirigés par l'industrie. Par exemple, dans son approche, l'Australie reconnaît qu'il y a transfert de confiance si une entité fait l'objet d'une certification croisée avec la stratégie nationale « *GATEKEEPER* » pour l'utilisation des clés publiques au gouvernement. (**http://www.gpka.gov.au/**)

[45] Certains pays ont adopté cette approche. Par exemple, en Australie, le « *National Electronic Authentication Council (NEAC)* » a été créé pour servir de centre national de liaison pour les questions d'authentification, chargé notamment de coordonner les activités qui y sont liées, à l'échelle nationale ou internationale, de donner des conseils au gouvernement et de suivre de près le développement des marchés. Font partie de ce conseil des représentants d'organismes importants qui s'intéressent au nouveau dossier de l'authentification (utilisateurs, organismes industriels ou gouvernementaux). (**http://www.dcita.gov.au/cgi-graphics/webdriver?MIval=dca_dispdoc&ID=4437**)

Est-il nécessaire d'organiser un nouveau forum à cette fin? Qui devrait établir ce forum? Qui devrait y participer? Quels rôles devront-ils jouer?

3.3 Principes de base de l'accréditation

Un ensemble de principes encadrera les éléments de base de l'accréditation des AC. Il est donc utile d'examiner des critères et modèles d'accréditation éventuels afin de déterminer quels seront les aspects (p. ex., rôles, responsabilités des divers intervenants, etc.) qui devront être pris en considération dans l'élaboration des principes.

Bien qu'il y ait diverses approches à l'accréditation, tous les modèles comporteront l'interaction d'une foule d'acteurs, chacun jouant un rôle ou un mélange de rôles. L'***Appendice B*** recense et nomme des rôles possibles. Même s'il est reconnu que ces rôles ne seront pas tous appropriés pour chaque modèle de fonctionnement et que d'autres rôles peuvent ne pas avoir été recensés, le modèle se veut un point de départ à partir duquel on peut voir comment les fonctions et les obligations des parties peuvent être réparties. C'est pourquoi il ne s'agit pas du modèle recommandé ou préféré, mais plutôt d'un exemple visant à fournir un cadre pour la discussion dans le contexte de l'élaboration des principes.

Toute forme d'accréditation consistera à veiller à ce que la politique de certification de l'AC satisfasse aux exigences liées à la sécurité, aux aspects juridiques et au rendement (énoncées dans les principes ou peut-être dans des normes). L'accréditation peut aussi confirmer (habituellement par une vérification indépendante) que les pratiques de l'AC élaborées et documentées dans l'énoncé des pratiques de certification sont conformes aux exigence des politiques de certification et (peut-être par des vérifications de conformité ou par le prélèvement de pénalités) faire en sorte que l'AC respecte les pratiques communiquées. Une approche encore plus élargie comporterait des mécanismes permettant aussi « d'accréditer » les mécanismes d'évaluation[46].

Il existe déjà sur le marché des outils qui servent de fondement à l'accréditation. Plus particulièrement, la partie 4 PKIX *Certificate Policy and Certification Practices*

[46] Toutefois, on laisse entendre que cela ne serait pas nécessaire si les évaluations étaient effectuées par des entités que l'on considère déjà comme dignes de confiance (p. ex., études d'avocats, cabinets comptables, etc.).

Framework (élaboré sous les auspices du Groupe IETF)[47] contient une liste de contrôle pour les exigences des politiques de certification (en ce qui concerne la génération et la révocation des certificats, la tenue des dossiers, etc.) et les aspects de l'énoncé de pratiques de certification (comme les exigences relatives à l'identité, la génération des clés, la délivrance du certificat, etc.). C'est un outil très utilisé en Amérique du Nord pour les initiatives d'accréditation.

Quels critères d'accréditation communs sont souhaitables? (Voir l'Appendice B pour un exemple de la façon dont les fonctions et les obligations peuvent être réparties dans les régimes d'accréditation.) Les rôles mentionnés à l'Appendice B sont-ils applicables et appropriés dans un environnement canadien? Où est-ce que votre organisation pourrait jouer un rôle (ou des rôles) dans ce modèle?

[47] « *Internet X.509 Public Key Infrastructure Policy and Certification Practices Framework* » **ftp://ftp.isi.edu/in-notes/rfc2527.txt**

Partie 4 - Développement des marchés : possibilités et défis

La définition d'un cadre pour les services d'authentification au Canada devrait être complétée par des initiatives visant la promotion de son développement et de son utilisation. La présente section repère les défis associés à la promotion de l'authentification et vise à recueillir des contributions sur les façons dont on pourrait élargir et accélérer l'adoption de techniques d'authentification efficaces. Elle porte également sur un éventail de mesures stratégiques qui peuvent permettre de surmonter les obstacles et de saisir les occasions offertes par ce marché. Enfin, en traitant de ces aspects, la présente partie soulève certaines questions qui devront être prises en compte dans l'élaboration des principes.

Compte tenu des contributions que les intervenants lui ont présentées jusqu'à présent, Industrie Canada est d'avis que les initiatives de développement des marchés devraient contribuer à :

- promouvoir l'adoption et l'utilisation de ces services par les entreprises et les consommateurs;
- favoriser la concurrence et promouvoir l'innovation en ce qui a trait aux technologies et aux applications;
- multiplier les possibilités pour les fournisseurs et les utilisateurs finaux, tant à l'échelle nationale qu'internationale.

4.1 Promouvoir l'adoption et l'utilisation

a) Investissement stratégique

Les entreprises devront comprendre que l'authentification électronique rend possible la communication interactive dans le contexte des réseaux ouverts. Les intervenants ont reconnu qu'il fallait inciter les entreprises à adopter à un point de vue prospectif et à reconnaître que des techniques d'authentification efficaces répondront aux attentes des utilisateurs quant à la façon dont la technologie peut améliorer leur vie.

Par conséquent, l'investissement à ce titre doit être présenté comme une mesure stratégique permettant aux entreprises de demeurer compétitives et, jusqu'à un certain point, d'anticiper la demande. Le plan d'action avant-gardiste de la Table ronde sur les possibilités des affaires électroniques canadiennes, qui vise à accélérer la participation du Canada à la cyberéconomie, a déjà offert des possibilités de faire connaître les avantages découlant de l'investissement dans

ce domaine[48]. En outre, la prise de mesures spécifiques ciblées à l'échelon des associations industrielles serait peut-être utile.

Les entreprises doivent non seulement reconnaître que cette technologie représente un investissement crucial du point de vue de la sécurité mais également comprendre qu'elle peut ajouter de la valeur à leurs processus opérationnels. En particulier, elles doivent réaliser que l'adoption de solides techniques d'authentification peut appuyer et faciliter de nouvelles applications et, par conséquent, procurer de nouvelles sources de revenus. C'est pourquoi les efforts promotionnels devraient chercher principalement à présenter la sécurité comme un catalyseur de nouveaux processus opérationnels. À cet égard, il serait bon qu'on établisse des profils et qu'on diffuse des exemples de réussite.

La viabilité économique des techniques d'authentification efficaces soulève des questions. Certains intervenants sont d'avis que cette technologie n'est tout simplement pas rentable, tandis que d'autres estiment que son caractère rentable se dévoilera avec le temps. Les tenants de cette dernière théorie sont persuadés qu'un bien plus grand nombre d'entreprises et de consommateurs se livreraient au commerce électronique s'ils avaient la certitude de pouvoir effectuer leurs transactions en toute sécurité. Ils pensent que la preuve de la rentabilité découlera de l'utilisation accrue.

Lorsqu'on sensibilisera les entreprises et qu'on les encouragera à investir dans cette technologie, il faudra qu'on insiste sur la nécessité d'une analyse approfondie des risques. Il est possible que le recours à des modèles de cadres d'évaluation ou à des cadres d'évaluation généraux soit utile en l'occurrence aux fins de l'élaboration de modèles de gestion des risques, en particulier dans le cas des petites entreprises pour lesquelles cette tâche est ardue. La réalisation de cette tâche pourrait être le fruit de la collaboration avec les associations industrielles.

Il faudra également qu'on se penche sur d'autres facteurs qui risquent de gêner l'investissement. Si l'on se fie aux structures de prix actuelles, le coût de l'adoption de cette technologie semble être l'un de ces facteurs. L'importance des frais d'entretien permanents entre également en ligne de compte. Il faudra donc qu'on incite les entreprises à étudier l'éventail des niveaux de sécurité disponibles de même que les approches « progressives » ou par étapes. Parallèlement, il faudra vraisemblablement que toute mesure stratégique visant à promouvoir l'adoption de cette technologie tienne compte des moyens de remanier les anciens systèmes pour assurer une authentification fiable. À ce propos, les fournisseurs auraient alors, semble-t-il, l'occasion de proposer des voies d'accès ou des « modes » d'authentification.

---

[48] Le plan d'action avant-gardiste de la Table ronde a prévu, à l'échelle régionale, une série d'événements régionaux de sensibilisation au commerce électronique et de promotion de son utilisation. La question de l'authentification a déjà été intégrée à certaines de ces activités. Pour de plus amples informations au sujet de ces événements, voir (**http://e-com.ic.gc.ca/equipe/evenements.html**).

Quelles mesures stratégiques faut-il adopter aux fins de la promotion des avantages des techniques d'authentification? Le secteur public pourrait-il prendre des mesures qui compléteraient les initiatives du secteur privé?

b) Sensibiliser les consommateurs au commerce électronique et les inciter l'utiliser

Pour ce qui est du consommateur (et souvent des petites et des micro entreprises), il sera peut-être plus difficile de mener à bien la tâche consistant à mieux renseigner les consommateurs et à faire en sorte qu'un plus grand nombre d'entre eux adoptent le commerce électronique. Les sondages menés auprès des consommateurs indiquent que ces derniers se préoccupent beaucoup de la protection de leur vie privée et, même s'ils sont disposés à essayer d'acheter des biens et des services, ils ne continueront à le faire que si leurs expériences d'achats préliminaires ont été faciles et réussies. Les nouvelles tendances statistiques indiquent que les consommateurs pratiquent en fait une certaine forme d'« équilibre » lorsqu'il s'agit de mener des activités en ligne. En ce qui concerne la protection de la vie privée, il semble qu'un grand nombre de consommateurs soient disposés à donner aux entreprises certains renseignements personnels en vue d'obtenir certains avantages (programmes de fidélisation, concours, etc.). Toutefois, avec l'adoption de la *Loi sur la protection des renseignements personnels et les documents électroniques*, ils peuvent maintenant le faire en sachant que des mesures de protection des renseignements personnels seront en place pour limiter l'usage et la divulgation de cette information, et que la surveillance par le Commissariat à la protection de la vie privée[49] fait partie de ces mesures. Pour ce qui est de la sécurité, de nombreux consommateurs ne comprennent pas les différentes techniques de sécurité disponibles et, par conséquent, acceptent l'application des mesures de sécurité actuelles pour des raisons associées au coût et à la commodité. Cependant, ces tendances sont largement fondées sur des observations générales. En ce moment-ci, le marché n'est pas encore bien informé sur la nature précise des compromis que les consommateurs sont disposés à faire sur le plan de la sécurité et de la protection de la vie privée.

Le fait que les consommateurs préfèrent les solutions transparentes rendra également l'opération plus ardue. Les consommateurs devront être plus ou moins familiers avec la technologie pour comprendre certains aspects de celle-ci et comparer les applications afin d'être en mesure de faire des choix éclairés en égard aux options offertes par les diverses autorités de certification. Même s'il n'existe pas encore de structures de prix pour ce marché, les consommateurs devront également se familiariser avec la technologie pour pouvoir faire le bon choix dans les circonstances où le coût entrera en ligne de compte. Signalons également qu'il faudra qu'on explique la fonction de non-répudiation qu'offre cette technologie. Le

---

[49] Dans certains cas, là où une législation de nature essentiellement semblable est adoptée au palier provincial, c'est cette dernière qui fournira la protection. Actuellement, la province de Québec est la seule province où la Loi fédérale a été supplantée par une législation provinciale.

nombre de transactions rejetées dans le contexte des réseaux ouverts nous porte à croire que cette option plaira aux consommateurs. Lorsqu'il est question de techniques d'authentification solides offrant la fonction de non-répudiation, il est important que toutes les personnes concernées soient parfaitement au courant de leurs propres droits et leurs responsabilités.

Il est possible qu'on doive également gérer d'autres aspects de l'acceptation par le consommateur. En particulier, les consultations auprès des intervenants ont révélé que ces derniers ont l'impression que le recours à l'authentification électronique donne la chance d'offrir aux consommateurs une meilleure protection - « améliore les choses » . Même si cela est le cas, il n'en reste pas moins que certaines responsabilités et imputabilités ne peuvent être ignorées. Par exemple, les utilisateurs doivent comprendre qu'ils sont tenus d'assurer la sécurité de leur clé privée. Étant donné que les consommateurs ont souvent l'impression qu'on leur demande d'assumer un nombre de responsabilités toujours croissant à mesure que la technologie évolue (p. ex., se rappeler de leur numéro d'identification personnel (NIP) et le garder secret sous peine d'être tenus responsables des transactions découlant d'une telle négligence), il se peut que le recours à des certificats numériques les laissent sceptiques. D'où l'importance qu'on mette en place des mécanismes d'atténuation du fardeau de la gestion des certificats et d'attribution équitable des responsabilités.

On croit généralement que les gouvernements doivent faire leur part pour mieux sensibiliser la population à leurs responsabilités et mieux la préparer à faire des choix liés à la protection des consommateurs. Les divers programmes offerts, dans le domaine du commerce électronique[50], par le BC, en collaboration avec d'autres organismes du secteur public ou avec le secteur privé, montrent que le gouvernement fédéral a déjà reconnu ce fait et qu'il a pris des mesures à cet égard. Comme nous l'avons déjà souligné, il est possible qu'on aborde la question de l'authentification en mettant en commun des ressources ou en travaillant conjointement avec d'autres organismes.

De quelle façon peut-on faire valoir aux yeux des gens d'affaires que l'authentification solide est un investissement stratégique? À qui peut-on confier cette tâche? Comment peut-on mieux sensibiliser les consommateurs aux avantages de l'authentification?

---

[50] Élaboration et diffusion de *Principes régissant la protection des consommateurs dans le commerce électronique : Le cadre canadien* (novembre 1999). Récemment, le BC a collaboré avec le secteur privé pour « opérationnaliser » ces principes et examiner des façons de faire en sorte que les programmes de sceaux respectent les principes et offrent aux consommateurs la confiance dont ils ont besoin pour magasiner en ligne. Le BC continue également de travailler avec les gouvernements provinciaux et territoriaux, les organisations de défense des consommateurs et l'industrie pour sensibiliser davantage les consommateurs et les éduquer.

c) Favoriser la concurrence et l'innovation

Les préoccupations liées à la concurrence sur les marchés électroniques sont comparables à celles qui se rattachent aux marchés traditionnels, abstraction faite d'un certain nombre de caractéristiques spéciales (p. ex., nouveaux rôles des intervenants, introduction d'intermédiaires, croissance rapide du marché, etc.). Dans le contexte des services d'authentification et de certification, il faudra suivre de près certains aspects de la concurrence qui peuvent se présenter[51]. Même si certains de ces aspects ont été traités à la partie 2 (Définition d'un programme axé sur l'avenir), d'autres touchent davantage les dimensions liées au développement du marché et seront traitées ci-après.

L'obligation qu'un consommateur doit obtenir l'« attestation » d'un certain organisme de certification avant de faire affaire avec une entreprise particulière, dans le contexte d'échanges commerciaux menés par la voie électronique entre une entreprise et un consommateur, préoccupait certains intervenants. Pour ce qui est des opérations interentreprises, on s'inquiétait de la possibilité que des entreprises soient exclues du processus des achats si elles n'utilisaient pas certaines technologies ou ne faisaient pas affaire avec certaines AC.

Dans le cas d'entreprises fournissant des produits ou des services à des consommateurs, les associations de défense des consommateurs ont fait remarquer que les AC ont la possibilité de jouer d'importants rôles sociaux étant donné qu'elles seront en mesure de retracer les données ayant trait aux activités commerciales[52]. Plus précisément, on a noté que les AC pourraient exercer beaucoup de pouvoir sur le marché en respectant le choix des particuliers puisqu'elles seront en mesure de délivrer et de révoquer les certificats. On a également souligné qu'une AC sera probablement en mesure de retracer toutes les personnes avec qui un particulier a effectué une transaction à l'aide d'une signature numérique particulière[53]. Si les entités qui agissent déjà à titre d'organisations de fiducie (p. ex. établissements financiers, associations comptables, organisations de défense des consommateurs, etc.) deviennent des AC, certaines protections et certaines garanties existeraient déjà, mais il se pourrait que des problèmes ayant trait aux politiques d'intérêt public surviennent dans le cas des nouveaux joueurs[54]. Même si

---

[51] Pour obtenir des renseignements sur le droit de la concurrence au Canada, voir (**http://strategis.ic.gc.ca/SSGF/ct01250f.html**). Pour obtenir des conseils sur le respect des dispositions législatives relatives à la concurrence, communiquer avec le Bureau de la concurrence.

[52] Il est possible que cela s'applique également à certaines applications interentreprises.

[53] Cette possibilité dépend de la façon dont les AC gèrent les listes de révocation. Selon la mise en oeuvre, Les AC utilisant une signature numérique peuvent vérifier la liste de révocation chaque fois. Au cours de la vérification de la liste, il est possible de créer une piste de données qui montrerait chaque demande de renseignements concernant ce certificat particulier.

[54] L'élaboration et l'application de principes axés sur le marché peuvent résoudre certains aspects importants de ces difficultés.

l'élaboration et l'application de principes axés sur le marché permettent de résoudre certains aspects importants de ces difficultés, il faut tout de même garder à l'esprit ces préoccupations.

Aussi, on a fait valoir que la conception de ces services était également une question d'intérêt public et qu'on devait mettre au point des services qui répondent aux besoins de tous les intervenants et non seulement aux besoins de ceux qui dominent le marché (p. ex., les prestataires de services). Cela nous autorise à penser que les gouvernements pourraient exercer une surveillance à cet égard, de même qu'en ce qui touche aux questions étroitement liées à l'établissement du prix des services.

À ce sujet, les intervenants ont évoqué la possibilité que les gouvernements jouent le rôle d'« arbitres » tout en prévenant qu'ils verraient d'un très mauvais oeil que l'innovation soit mise en péril, soit en bloquant artificiellement l'accès au marché, soit en tolérant que des concurrents attitrés créent des difficultés qui désavantageraient leurs rivaux innovateurs. Il faut également qu'on prévienne les abus de pouvoir par lesquels les intervenants du secteur privé pourraient faire obstacle au développement ou à l'essor du marché en adoptant, collectivement ou individuellement, des pratiques limitatives.

Lorsqu'on examine de près les aspects de la concurrence, on doit s'assurer que le marché soutient l'innovation et l'investissement. On croit que l'élaboration, par le secteur privé, de normes pratiques du point de vue commercial peuvent contribuer, dans une large mesure, à la réalisation de cet objectif en établissant des règles équitables, à condition que ces normes soient le reflet d'un accord consensuel entre les intervenants et qu'elles n'étouffent pas la concurrence et l'innovation. Toutefois, l'innovation étant une force positive du point de vue de la concurrence, on doit veiller à ce que les normes ne l'étouffent pas.

Est-il nécessaire de prendre des mesures spéciales pour garantir la concurrence et favoriser l'innovation dans ce marché? Certains aspects de la concurrence posent-il des problèmes devant être définis et suivis?

Partie 5 : Conclusions et prochaines étapes

Il faut être attentif aux nombreux aspects de la tâche à accomplir et à ses multiples éléments interdépendants. À mesure que progressent les efforts visant à mettre au point une stratégie canadienne, on devra toujours tenir compte de ces aspects et de ces éléments ainsi que des mesures et des efforts de travail qui y sont liés, tant sur le plan national qu'international. Dans le présent document, nous avons tenté de réunir de l'information sur ces considérations encore qu'il se produise chaque jour des faits nouveaux dans ce milieu en constante évolution. Dans cet esprit, il faudra qu'on prenne le taureau par les cornes et qu'on se tienne au courant de la suite des événements dans les secteurs public et privé pour garantir que les orientations prises correspondent aux tendances mondiales qui se dessinent dans ces secteurs.

5.1 Prochaines étapes proposées

La prochaine étape consistera pour les secteurs public et privé à collaborer sur les points suivants :

i) Établir et mettre à exécution un mode de définition d'une série de principes communs axés sur le marché qui s'appliqueraient au Canada aux fins des services d'authentification et de certification.

ii) Planifier et mettre en oeuvre des mesures stratégiques visant à promouvoir, auprès des entreprises et des utilisateurs finals, le recours à de solides techniques d'authentification.

iii) Continuer de travailler sur le plan international pour influer sur les orientations et veiller à ce que le Canada soit bien positionné pour profiter pleinement des possibilités offertes par ce marché.

Le dialogue ininterrompu entre les secteurs public et privé qui, aux yeux des intervenants, est indispensable à la progression du dossier de la confiance au Canada, sera également important du point de vue de l'élaboration réussie d'une stratégie. À l'étape suivante de ce dialogue, les groupes d'intervenants sont priés de répondre à l'une ou l'autre ou à l'ensemble des questions dont il est fait état dans le présent document (page ii, en début de document). *L'**Appendice C*** rassemble ces questions au sujet desquelles les intervenants donneront leurs opinions et leurs commentaires. Ils sont également priés de faire part de leurs observations relativement au sommaire des éventuels rôles qui figure à l'***Appendice D.***

Appendice A

Programme de consultation sur l'authentification : Intervenants participant

AEPOS Technologies Corporation
Alliance des manufacturiers et des exportateurs du Canada
Association canadienne de la technologie de l'information (ACTI)
Association canadienne des compagnies d'assurances de personnes inc. (ACCAP)
Association canadienne des fournisseurs Internet (ACFI)
Association canadienne des paiements (ACP)
Association des banquiers canadiens (ABC)
Association des consommateurs du Canada (ACC)
Banque Canadienne Impériale de Commerce (Identrus)
Banque de Montréal (MBANX)
Banque de Nouvelle-Écosse
Banque Royale
BCE Emergis Inc.
Bell Canada
British Columbia Technology Industries Association
Bureau du commissaire à la protection de la vie privée du Canada
Canadian Marketing Association (CMA)
Centre pour la défense de l'intérêt public (CDIP)
Coalition canadienne de la santé
Conseil canadien du commerce de détail (CCCD)
Conseil canadien des normes (CCN)
Conseil canadien pour le commerce international (CCCI)
DataPrivacy Partners Ltd.
Deloitte & Touche
Electronic Commerce Canada
Entrust Technologies Ltd.
Ernst & Young
Fédération canadienne de l'entreprise indépendante (FCEI)
Institut canadien des comptables agréés (ICCA)
IBM Canada limitée
KPMG
Milieu universitaire (Université Dalhousie, Université d'Ottawa)
Mondex Canada
Nortel Networks
Option consommateurs
Provinces (Columbie-Britannique, Nouveau-Brunswick, Ontario, Québec)
Société canadienne des postes
Sprint Canada
Vérificateur général
VISA Canada Association

Appendice B

Cadre proposé en vue de la discussion sur le ou les modèles d' accréditation

Fonctions liées à l'accréditation et interaction

Même si la terminologie varie d'un secteur de compétence international à l'autre, on reconnaît de plus en plus que l'accréditation des autorités de certification (CA) nécessite l'interaction des intervenants, des entités juridiques, des parties, des intéressés, des organismes ou des représentants remplissant les fonctions suivantes :

Autorité compétente – Il s'agit du représentant d'un secteur de compétence juridique ou d'une communauté d'intérêt. Cette personne assume la responsabilité, au sein du secteur de compétence ou de la communauté d'intérêt, d'un certain nombre d'actes pouvant comprendre tous ceux qui suivent ou certains d'entre eux :

- Définir le contexte politique et juridique dans lequel le programme sera exécuté.
- Négocier avec d'autres *autorités compétentes* pour garantir l'harmonisation entre les secteurs de compétence juridique.
- Délivrer des permis, des autorisations ou d'autres marques de reconnaissance gouvernementale ou juridique aux diverses AC et élaborer des règles à leur intention.
- Fixer des exigences minimales pour que soit favorisées la compatibilité des niveaux de confiance de la signature numérique et l'approche d'accréditation des AC dans tous les secteurs de compétence juridique.
- Accorder une reconnaissance formelle aux normes, aux critères et aux plans visant à favoriser la compatibilité des niveaux de confiance de la signature numérique et l'approche d'accréditation dans tous les secteurs de compétence juridique.
- Ratifier l'approche d'accréditation et lui conférer la reconnaissance officielle.
- Conférer la reconnaissance officielle à l'*organe d'accréditation des évaluateurs rattachés à un AC*.

Organe d'accréditation des évaluateurs rattachés à une autorité de certification – Il s'agit d'une organisation indépendante, d'une association industrielle ou d'un autre organisme pouvant être reconnu par l'*autorité compétente* ou pouvant fonctionner sur la base de relations de confiance établies avec des *évaluateurs rattachés à une AC* ou des *instances directrices*. Cette organisation doit :

- Attester que les *évaluateurs rattachés à une AC* ont la compétence professionnelle voulue pour mener des évaluations conformément aux

politiques de certification ou à d'autres exigences pouvant être fixées par l'*autorité compétente*.

- Sanctionner, sélectionner ou élaborer des directives, des critères et des normes ayant trait au respect des lignes de conduite.

Évaluateur rattaché à une autorité de certification – Il s'agit d'un représentant indépendant, membre d'un organisme responsable, ou d'un autre professionnel compétent ayant la confiance de l'*instance dirigeante*. Il se peut que l'*évaluateur rattaché à une AC* soit officiellement reconnu par un *organe d'accréditation des évaluateurs rattachés à une autorité de certirfication* s'il en existe un dans le secteur de compétence ou la communauté d'intérêt en question. Cette personne doit :

- Déterminer si *l'instance opérationnelle* respecte la *politique de certification*.
- En se fondant sur certains critères, directives ou normes élaborés aux fins de l'évaluation et sanctionnés par l'*organe d'accréditation*, se faire une « opinion de vérificateur » au sujet des points suivants :
  - **1)** Pertinence des contrôles mis en place.
  - **2)** Fonctionnement efficace de ces derniers, de sorte qu'on puisse être certain que les transactions sont inscrites, traitées, exécutées ou tenues par l'*instance opérationnelle* en question.
- Évaluation d'autres éléments qui prouvent qu'on respecte la *politique de certification* visée dans les cas où les parties donnent suite à des obligations découlant de certains mécanismes (comme des contrats ou des conventions d'affiliation) ou de la mise en oeuvre de mesures de sauvegarde opérationnelles ou de méthodes de gestion connexes. Il n'est pas nécessaire que de la documentation ayant trait à ces mécanismes ait été directement jointe à *l'énoncé des pratiques de certification*. Eu égard à certaines exigences de la *politique de certification*, il se peut que *l'évaluateur rattaché à une AC* n'ait besoin que d'une référence externe pour évaluer les pratiques pertinentes concernant le domaine de la communauté fermée de l'AC.
- Rédaction d'un *rapport d'évaluation de la conformité à la politique de certification*. Au nombre des éventuels lecteurs de ce compte rendu, mentionnons:
  - **a)** **Les parties concernées** qui s'intéressent vivement au fait que des pratiques répondent ou non aux exigences de la *politique de certification*.
  - **b)** **Les abonnés** qui veulent savoir si l'AC satisfait aux exigences de la politique de certification.

c) **Les autorités compétentes** - La vérification est un volet important de n'importe quel mécanisme d'approbation, de réglementation, d'octroi de permis ou d'une autre forme de reconnaissance. L'*autorité compétente* se sert du rapport d'évaluation dans le contexte du processus initial et continu de reconnaissance.

d) **Les instances dirigeantes** sont les principales utilisatrices du rapport d'évaluation, car l'évaluation est l'une des exigences de la politique de certification ciblée et elle démontre que l'AC respecte cette politique. Les instances dirigeantes se serviront également du rapport d'évaluation dans le contexte de toute négociation axée sur l'intercertification.

e) **Les instances opérationnelles.** Même si le rapport d'évaluation ne vise pas à fournir des recommandations en vue du perfectionnement des contrôles internes d'une autorité de certification, il renferme souvent des observations relatives à l'amélioration des opérations, ce qui constitue un avantage supplémentaire.

Responsable de l'accréditation de sécurité – Il s'agit du représentant du domaine ou du secteur de l'AC qui doit :

- Approuver le mode de fonctionnement d'un organisme de certification fondé sur le recours à des mesures de sécurité particulières.
- Assumer les risques résiduels liés à la sécurité pour le compte du domaine ou du secteur de l'AC.

Instance dirigeante – Il s'agit du représentant du domaine ou du secteur de l'AC. L'*instance dirigeante* doit :

- Sélectionner ou définir la documentation devant être utilisée dans le domaine ou le secteur organisationnel de l'organisme de certification.
- Approuver tout accord d'intercertification ou d'interopérabilité conclu avec les représentants d'autres domaines.
- Approuver les pratiques que l'AC doit suivre en passant en revue l'énoncé des pratiques de certification pour garantir qu'il est conforme aux lignes politiques de certification.
- Fournir une orientation de principe à l'*instance opérationnelle*.

Instance opérationnelle – Il s'agit d'un représentant du domaine ou du secteur de l'AC. Dans certains modèles de gestion, il peut y avoir plusieurs instances opérationnelles qui participent au processus de délivrance d'un certificat. Dans la plupart des cas, tous les éléments sont accrédités pour que soit atteint le niveau de confiance nécessaire aux fins de la délivrance d'un certificat en particulier. L'*instance opérationnelle* doit rendre compte à l'*instance dirigeante* de l'exécution des tâches suivantes :

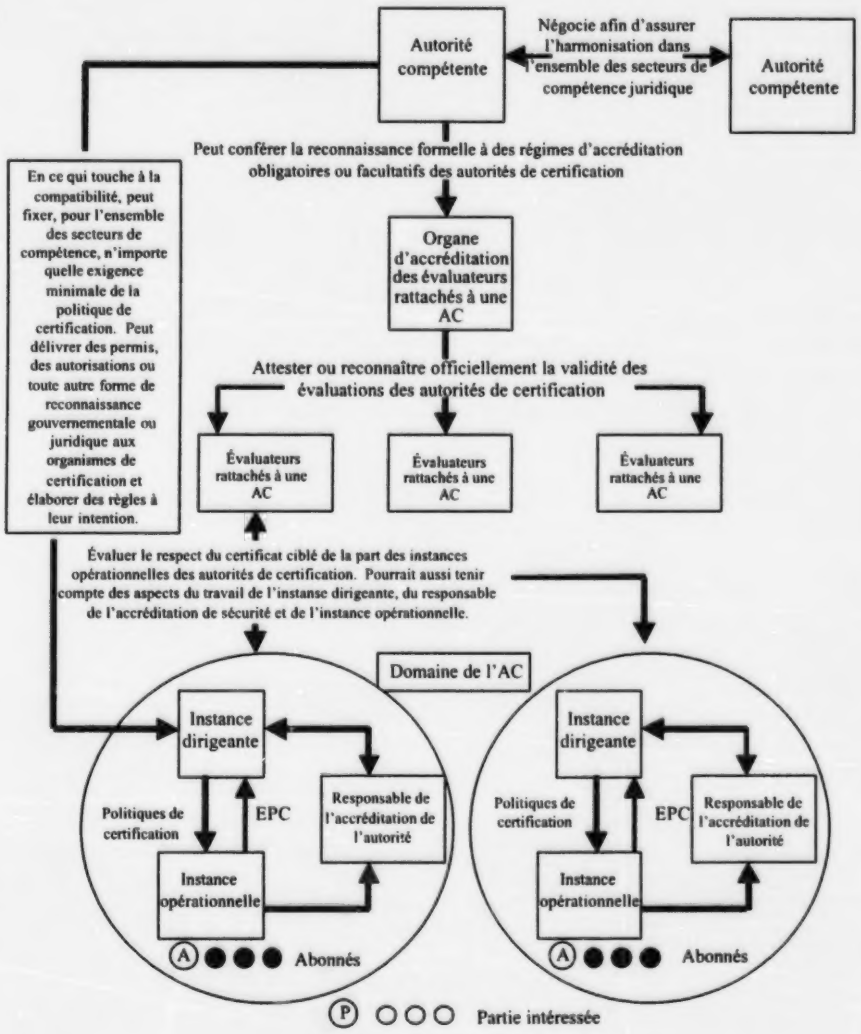
- Interpréter les politique de certification qui ont été sélectionnées ou définies par l'*instance dirigeante*.
- Élaborer les pratiques relatives à la documentation de la conformité aux politiques ou autres exigences.
- S'assurer que les énoncés des pratiques sont mis à jour au besoin.
- Faire en sorte que le fonctionnement de l'organisme de certification ou du programme soit conforme aux énoncés des pratiques.

Abonné – Il s'agit d'un membre du domaine de l'AC. Cette personne, qui est visée par le certificat, est en mesure d'utiliser et est autorisé à utiliser la clé privée qui correspond à la clé publique du certificat. Les responsabilités et les obligations de l'*abonné* sont définies dans la ligne directrice de l'AC.

Partie intéressée - Peut être ou non un *abonné* du même domaine. On a attribué à la *partie intéressée* un certificat, sur la foi duquel elle se fonde pour agir, ou des signatures numériques qui sont vérifiées grâce à ce dernier.

Cadre d'accréditation

Le diagramme suivant illustre les liens entre les diverses fonctions. La combinaison de celles-ci permet d'élaborer des modèles d'accréditation uniques des autorités de certification (AC) qui tiennent compte des besoins du secteur de compétence juridique ou des modèles de gestion (ouverts ou fermés), ou des deux.



© Industrie Canada et LGS conseillers en informatique inc. 1999. Tous droits réservés.

Appendice C

Liste récapitulative des questions

Un cadre pour les services d'authentification et de certification - Approche proposée

Principes

1) Comment les travaux en cours et les documents existants peuvent-ils être adaptés à l'élaboration de principes au Canada?

2) Dans quelle mesure les principes devraient-ils influer sur les modalités des contrats qui régiront les services relatifs à l'authentification dans des environnements fermés? Dans quelles circonstances conviendrait-il de varier les aspects de mise en oeuvre des principes?

3) Sur quels autres domaines les principes devraient-ils porter? Et pourquoi?

4) Comment traiter la question du respect? Dans quelles circonstances est-il souhaitable d'avoir une certaine forme d'évaluation ou de vérification des principes? Qui devrait assurer la fonction d'évaluation? En fonction de quels critères? Que se passe-t-il si l'on fait reposer la conformité sur les autodéclarations? Dans quelles circonstances conviendrait-il de dériver les assurances nécessaires des relations avec les entités existantes dignes de confiance?

5) Est-il nécessaire d'organiser un nouveau forum à cette fin? Qui devrait établir ce forum? Qui devrait y participer? Quels rôles devront-ils jouer?

Principes de base de l'accréditation

6) Quels critères d'accréditation communs sont souhaitables? (Voir l'Appendice B pour un exemple de la façon dont les fonctions et les obligations peuvent être réparties dans les régimes d'accréditation.) Les rôles mentionnés à l'Appendice B sont-ils applicables et appropriés dans un environnement canadien? Où est-ce que votre organisation pourrait jouer un rôle (ou des rôles) dans ce modèle?

Développement des marchés : possibilités et défis

7) Quelles mesures stratégiques faut-il adopter aux fins de la promotion des avantages des techniques d'authentification? Le secteur public pourrait-il prendre des mesures qui compléteraient les initiatives du secteur privé?

8) De quelle façon peut-on faire valoir aux yeux des gens d'affaires que l'authentification solide est un investissement stratégique? À qui peut-on confier cette tâche? Comment peut-on mieux sensibiliser les consommateurs aux avantages de l'authentification?

9) Est-il nécessaire de prendre des mesures spéciales pour garantir la concurrence et favoriser l'innovation dans ce marché? Certains aspects de la concurrence posent-il des problèmes devant être définis et suivis?

Appendice D

Sommaire des rôles éventuels des secteurs public et privé

Secteurs public et privé

- Promouvoir l'utilisation des services d'authentification et des services connexes en tant que base éprouvée et sécuritaire du commerce électronique.
- Faire connaître les avantages de la technologie et faire en sorte que les utilisateurs soient plus sensibilisés à celle-ci et qu'ils la comprennent mieux.
- Renseigner les consommateurs et les entreprises sur la technologie et sur ses avantages.
- Établir une approche commune en matière d'accréditation des autorités de certification.

Secteur privé

- Perfectionner et mettre en application des programmes d'accréditation.
- Concevoir une série générale de principes ayant trait au marché.
- Collaborer aux activités internationales visant à garantir que l'approche canadienne est compatible avec les orientations mondiales et que les certificats canadiens sont reconnus dans tous les pays.
- Assumer le leadership en mettant au point des produits qui répondent aux besoins des utilisateurs.
- Transmettre rapidement aux administrations canadiennes des observations sur les objectifs et les stratégies d'orientation.
- Élaborer des normes (au besoin) pour étayer les principes et favoriser l'interopérabilité.

Secteur public

- Faciliter le dialogue sur les approches nationales qui font le lien avec les approches internationales.
- Soutenir le programme d'élaboration de principes.
- Assurer la coordination avec les provinces.
- Surveiller les aspects de la concurrence (et prendre les mesures qui s'imposent au besoin).
- Être un utilisateur modèle (p. ex., ICP-GC)

- Encourager le dialogue et l'établissement de liens avec le monde universitaire.
- Protéger les intérêts canadiens (s'assurer que l'approche adoptée, quelle qu'elle soit, rend possible, pour les entreprises et les consommateurs canadiens, l'interopérabilité à l'échelle internationale).
- Mettre aux point des mesures préliminaires (en cas d'échec des solutions du secteur privé).

Liste des abréviations

ABA	American Bar Association
AC	Autorité de certification
AGB	Alliance of Global Business
APEC	Organisation de coopération Asie-Pacifique (APEC)
API	Agents principaux de l'information
BC	Bureau de la consommation (Industrie Canada)
BIAC	Business and Industry Advisory Committee (to the OECD)
CARAT	Certification Authority Rating and Trust
CCE	Commission des Communautés européennes
CNUDCI	Commission des Nations Unies pour le droit commercial international (CNUDCI)
CHLC	Conférence pour l'harmonisation des lois au Canada
CDPISP	Conseil des Dirigeants principaux de l'information du secteur public
DPI	Dirigeants principaux de l'information
E.U.	États-Unies
GBDe	Global Business Dialogue on Electronic Commerce
GC	Gouvernement du Canada
ICP	Infrastructure à clé publique
ICP-GC	Infrastructure à clé publique du gouvernement du Canada
IETF	Internet Engineering Task Force
ILPF	Internet Law and Policy Forum
NACHA	National Automated Clearing House Association
NEAC	National Electronic Authentication Council (Australia)
NIP	Numéro d'identification personnel
OCDE	Organisation de coopération et de développement international (OCDE)
PKIX	Public Key Infrastructure (X.509)
UE	Union européenne

Sources choisies

Sources nationales -Contexte

- *Le ministre Manley présente les grandes lignes de la politique du Canada en matière de cryptographie*, Industrie Canada, octobre 1998

  http://e-com.ic.gc.ca/francais/releases/41d6.html

- *Notes pour une allocution de l'honorable John Manley, ministre de l'Industrie au cercle national des journalistes du Canada - La politique du Canada en matière de cryptograhie*, Industrie Canada, octobre 1998

  http://e-com.ic.gc.ca/francais/speeches/42d3.html

- *Résumé de la politique du Canada en matière de cryptographie*, Industrie Canada

  http://e-com.ic.gc.ca/francais/fastfacts/43d7.html

Sources nationales - Programme de consultation mené par la Direction générale du commerce électronique

- *Authentification électronique : consultations bilatérales - sommaire des conclusions*, octobre 1999

  http://ecom.ic.gc.ca/francais/documents/bilat-fr.pdf

- Documentation relative à l'Atelier sur les politiques en matière d'authentification électronique, tenu le 6 décembre 1999 :

  - Ordre du jour

    http://ecom.ic.gc.ca/francais/documents/ordredujour.pdf

  - Résumé de la rencontre

    http://ecom.ic.gc.ca/francais/documents/résumé-atelier.pdf

  - Documents de travail

    http://ecom.ic.gc.ca/francais/documents/documents-tra.pdf

Sources nationales - Documentation et liens connexes

- « *Approaches to Authentication* », AEPOS Technologies Corporation, décembre 1999.

- *Déclaration conjointe Canada-Australie sur le commerce électronique mondial*, les gouvernements de l'Australie et du Canada, février 2000

  http://ecom.ic.gc.ca/francais/releases/41d12.html

- *Loi sur la protection des renseignements personnels et les documents électroniques*, Industrie Canada, avril 2000

  http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-F.html

- L'Institut Canadien des Comptables Agréés (ICCA) (À propos de WebTrust)

  http://www.cica.ca/cica/cicawebsite.nsf/public/Aproposdeswebtrust

- « *Certification and Accreditation for PKIs and Certification Authorities - Survey of Standards, Trends and Identification of Potential Models* », Domus Software Limited/Industrie Canada, août 1998.

- Ministère de la Justice Canada (Programmes et services - Commerce électronique)

  http://www.canada.justice.gc.ca/fr/ps/ce/index.html

- *Déclaration conjointe de l'Union européenne et du Canada : Le commerce électronique dans la société de l'information mondiale*, l'Union européenne et le gouvernement du Canada, décembre 1999

  http://ecom.ic.gc.ca/francais/71ta.html

- *L'Infrastructure à clé publique (ICP) du gouvernement du Canada (GC)*, Secrétariat Conseil du Trésor

  http://www.cio-dpi.gc.ca/pki/initiatives/initiatives_f.html

- *Principes régissant la protection des consommateurs dans le commerce électronique - Le cadre canadien* (et documents connexes), Bureau de la consommation, Industrie Canada, novembre 1999

  http://strategis.ic.gc.ca/SSGF/ca01180f.html

- Conseil des dirigeants principaux de l'information du secteur public (CDPISP)

  http://www.tbs-sct.gc.ca/cio-dpi/pscioc/pscioc_home_f.html

- *Pour une progression rapide : Comment faire du Canada un leader dans l'économie sur Internet*, Rapport de la Table ronde sur les possibilités des affaires électroniques canadiennes, The Boston Consulting Group (Canada), janvier 2000

  http://www.bcg.com/practice/francais.asp# et/ou
  http://e-com.ic.gc.ca/equipe/ressources.html#rap

- *Loi uniforme sur le commerce électronique*, Conférence pour l'harmonisation des lois au Canada

  http://www.law.ualberta.ca/alri/ulc/findex.htm

Sources internationales - Documentation et liens connexes

- Business and Industry Advisory Committee to the OECD (BIAC)

  http://www.biac.org/

- « *Digital Signature Guidelines* », Information Security Committee, Section of Science and Technology », American Bar Association, août 1996

  http://www.abanet.org/scitech/ec/isc/dsgfree.html

- *Directive sur un cadre communautaire pour les signatures électroniques,* le Parlement européen et le Conseil de l'Union européenne, décembre 1999

  http://www.ispo.cec.be/Ecommerce/legal/documents/1999_93/1999_93_fr.pdf

- *Projet de règles uniformes sur les signatures électroniques*, CNUDCI, décembre 1999

  http://www.uncitral.org/fr-index.htm

- Global Business Dialogue on Electronic Commerce (GBDe)

  http://www.gbd.org/

- Union internationale des télécommunications

  http://www.itu.int/index-fr.html

- International Chamber of Commerce (ICC)

  http://www.iccwbo.org/index.asp

- Internet Law & Policy Forum (ILPF)

  http://www.ilpf.org/

- « *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* » The Internet Engineering Task Force, mars 1999

  ftp://ftp.isi.edu/in-notes/rfc2527.txt

- « *Inventory of Approaches to Authentication and Certification in a Global Networked Society* », OCDE, octobre 1999

  http://www.olis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg(99)13-final

- « *Issues Relating to the Use of Electronic Authentication* », Electronic Authentication Task Group, APEC Telecommunications Working Group

  http://www.apii.or.kr/telwg/eaTG/eaTG-2.htm

  Appendices

  http://www.apii.or.kr/telwg/eaTG/eaTG-cont.html

- Joint OECD-Private Sector Workshop on Electronic Authentication, juin 1999.

  http://www.oecd.org/dsti/sti/it/index.htm

- PKI (Public-Key Infrastructure) Forum »

  http://www.pkiforum.org/

- *Déclaration des ministres sur l'authentification pour le commerce électronique*, OCDE, octobre 1998

  http://appli1.oecd.org/olis/1998doc.nsf/e8937a71740f342a8025656400591559/90270c904b319965c12566dd003230fd/$FILE/12F89557.FRE

- « *The Global Action Plan for Electronic Com0merce* », The Alliance for Global Business (AGB), Global Information Infrastructure Commission (GIIC) **http://www.gii.org/focus/ecommerce/agbecplan.html**